IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re:	David J. Wetherall	Confirmation No:	1582
Application No:	09/825,139	Group:	2153
Filed:	April 3, 2001	Examiner:	Barqadle, Yasin M.
For:	Independent Detection and Filtering of Undesirable Packets		
Customer No.:	29127		
Attorney Docket No.	0016.0007US1		

APPELLANTS' BRIEF

VIA FACSIMILE: **571-273-8300**
Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450,
Alexandria, Virginia 22313-1450

Sir:

This is the Applicants' appeal from the final Office Action, mailed February 6, 2007 (Paper No. 20070201).

A three-month extension of time is requested for this response.

Real Party in Interest

Arbor Networks, Inc. is the real party in interest.

Related Appeals and Interferences

There are no related appeals or interferences.

Status of Claims

Claims 1-9, 11-13, 17-25 and 32 are pending in the application. Claims 1-9, 11-13, 17-25 and 32 are rejected. Claim 10, 14-16, and 26-31 are cancelled. Claims 1-9, 11-13, 17-25 and 32 are being appealed.

Status of Amendments

All amendments have been entered. There were no post final amendments or proposed amendments.

Summary of Claimed Subject Matter

Claim 1 is directed to a method of operation in a routing device. See originally filed drawings of instant application (Drawings) at Fig. 2 and Fig. 1, reference numeral 108 and the originally filed specification of the instant application (Specification) at page 5, line 12.

A packet sent by a client device is received by the routing device. See Drawings at Fig. 8, and Specification at page 12, line 5.

The routing device determines if the packet is destined for a server of interest by reference to a destination address of the packet. See Drawings at Fig. 8, reference numeral 802, and Specification at page 12, line 5.

If not destined for the server of interest, the packet is routed to its destination. See Drawings at Fig. 8, reference numeral 804, and Specification at page 12, lines 9-10.

If the packet is determined to be destined for the server of interest, however, the router independently determines whether the packet is a part of a conversation between the client device and the server of interest based at least in part on persistent information included in the packet. See Drawings at Fig. 8, reference numerals 806, 808, 810, and Specification at page 12, lines 11-24.

The packet is handled based at least in part on the result of the independent determination by forwarding the packet to the server of interest if the packet is deemed to

be a part of a conversation between the client device and the server. See Drawings at Fig. 8, reference numeral 812, and Specification at page 12, lines 24-25. On the other hand, the packet is dropped if the packet is deemed to be an undesirable packet. See Drawings at Fig. 8, reference numeral 814, and Specification at page 13, lines 1-4.

Dependent claim 2 requires that the independent determination comprises independently verifying a conversation identifier included in the packet based at least in part on other information included in the packet. Further, depending claim 3 requires that independent verification comprises independently regenerating the conversation identifier using at least other information included in the packet and comparing the independently re-generated conversation identifier with the included conversation identifier. See generally, Drawings at Fig. 8, reference numerals 806, 808, 810, and Specification at page 12, lines 11-24.

Independent claim 11 is directed to method of operation in a server and network. See Drawings at Fig. 2 and Fig. 1, and Specification at page 5, line 8-11.

Independently verifiable conversation identifiers are generated for a packet destined for a client device, using at least persistent information that will be included in the packet. See Drawings at Fig. 3, reference numeral 302, and Specification at page 8, lines 15-16.

The independently verifiable conversation identifier is included with the packet for use by the client device to include in a subsequent packet sent by the client device destined for the server. See Drawings at Fig. 3, reference numeral 304, and Specification at page 9, lines 17-18.

The independently verifiable conversation identifier included in the packet is transmitted to the client device. See Drawings at Fig. 3, reference numeral 306, and Specification at page 8, lines 18-19.

The routers determine whether to forward or drop the packet through a network in response to the conversation identifier to protect the network against undesirable packets by determining if the packet is destined for the server by reference to a destination address of the packet (see Drawings at Fig. 8, reference numeral 802, and Specification at page 12, line 5), if the packet is not destined for the server routing the packet to its destination (see Drawings at Fig. 8, reference numeral 804, and Specification at page 12, lines 9-10), if the packet is determined to be destined for the server determining whether the packet is a part of a conversation between the client device and the server based at least in part on the included persistent information and forwarding the packet to the server if the packet is deemed to be a part of a conversation between the client device and the server (see Drawings at Fig. 8, reference numerals 806, 808, 810, and Specification at page 12, lines 11-24) and dropping the packet if the packet is deemed to be an undesirable packet (see Drawings at Fig. 8, reference numeral 814, and Specification at page 13, lines 1-4).

Claim 17 concerns a routing apparatus. See Drawings at Fig. 9.

An interface receives a packet sent by a client device destined for a server. See Drawings at Fig. 8, and Specification at page 12, line 4.

A function unit coupled to the interface independently determines whether the packet is a part of a conversation between the client and the server based at least in part on persistent information included in the packet, and outputs a packet disposition signal based at least in part on the result of the independent determination. See Drawings at Fig. 9, reference numeral 908, and Specification at page 14, line 15-26.

The function unit determines if the packet is destined for the server by reference to a destination address of the packet; if the packet is not destined for the server, the packet is routed to its destination (see Drawings at Fig. 8, reference numeral 802, and Specification at page 12, line 5). If the packet is determined to be destined for the server, it independently determines whether the packet is a part of a conversation between the

client device and the server based at least in part on the persistent information included in the packet (see Drawings at Fig. 8, reference numerals 806, 808, 810, and Specification at page 12, lines 11-24); wherein the packet disposition signal causes the routing device to forward the packet to the server if the packet is deemed to be a part of conversation between the client device and the server and drop the packet if the packet is deemed to be an undesirable packet (see Drawings at Fig. 8, reference numeral 814, and Specification at page 13, lines 1-4).

Claim 22 concerns a server comprising at least one processor and a communication interface coupled to the processor to transmit packets to one or more client devices on behalf of the processor. See Drawings at Fig. 4, and Specification at page 8, lines 11-14.

A generator generates an independently verifiable conversation identifier for a packet destined for one of the one or more client devices, using at least persistent information that will be included in the packet. A summing unit inserts the independently verifiable conversation identifier with the packet for use by the particular client device to include in a subsequent packet sent by the client device destined for the server. See Drawings at Fig. 4, reference numeral 408, and Specification at page 10, lines 3-10. A transmitter transmits the independently verifiable conversation identifier included packet to the particular client device. See Specification at page 10, lines 4.

A router determines if the packet is destined for the server by reference to a destination address of the packet (see Drawings at Fig. 8, reference numeral 802, and Specification at page 12, line 5); if the packet is not destined for the server, the packet is routed to its destination (see Drawings at Fig. 8, reference numeral 804, and Specification at page 12, lines 9-10). If the packet is determined to be destined for the server, there is an independent determination of whether the packet is a part of a conversation between the client device and the server based at least in part on the independently verifiable conversation identifier included in the packet. The routing device forwards the packet to the server if the packet is deemed to be a part of the conversation between the client

device and the server (see Drawings at Fig. 8, reference numerals 806, 808, 810, and Specification at page 12, lines 11-24) and drops the packet if the packet is deemed to be an undesirable packet (see Drawings at Fig. 8, reference numeral 814, and Specification at page 13, lines 1-4).

Grounds of Rejection to be Reviewed on Appeal

Claims 1-3, 10-11, 17-19, 22 and 32 were rejected under 35 U.S.C. 103(a) as being unpatentable over Primak *et al.* (USPN 6,598,077) (Primak Patent) in view of Canion *et al.* (U.S. Published Application Publication No. 2002/0108059) (Canion Application).

Claims 4-9, 12-13, 20, 21, and 23-25 were rejected under 35 U.S.C. 103(a) as being unpatentable over the Primak Patent in view of the Canion Application and further in view of Bull *et al.* (USPN 6,799,270) (Bull Patent).

Argument

Scope and content of the applied references

The Primak Patent concerns the infrastructure behind web sites and deals with the scaling of web site databases and handling requests for dynamic content. For example, in the Primak system, incoming client requests for dynamic content are sent to a dynamic content router 10. See Primak Patent at col 6, line 61. The Primak content router 10 then selects an application server 10. See Primak Patent at col. 6, lines 64. This selection is based, for example, on the particular content requested. See Primak Patent at col. 5, line 60-col. 6, line 8.

The client assignment to a particular application server is maintained using a Session ID. See Primak Patent at col. 8, lines 24-26. The content router routes incoming client requests based upon the Session ID contained in those requests. See Primak Patent at col. 8, lines 45-48.

In this way, the Primak Patent is directed to a system for managing and distributing work over a web site system.

The Canion Application is directed to a hardware device termed a "security accelerator". See Canion Application at paragraph [0010]. Packets coming into the system are analyzed to determine whether they represent a security violation, part of a denial of service attack, or not. See Canion Application at paragraph [0183]. Packets that are determined to represent no threat are simply passed-through to an associated subsystem. See Canion Application at paragraph [0183]. .

The Bull Patent is directed to a system for securely distributing session keys to computer nodes connected in a chain. A nested request is serially generated by the chained nodes and submitted to an authentication server, which authentication server then issues a session key to each node in the chain.

Arguments relative to whether claims 1, 11, 17, and 22 are unpatentable over Primak Patent in view of Canion Application:

Claim 1, for example, is directed to a system for protecting certain servers, "server of interest" in the parlance of the claim, from undesirable packets, such as those packets generated in a denial of service attack, for example. Independent claims 11, 17, and 22 have similar features.

The system of claim 1 functions by first determining of the packet is destined for a server of interest by reference to a destination address. When the packet is not destined from that server of interest, it is simply forwarded. On the other hand, when the packets are destined for the server of interest, the method includes determining whether the packet is part of a conversation by reference to persistent information and then forwarding or dropping the back based on whether the packet is part of the conversation or not.

Independent claims 11, 17, and 22 have similar features: monitoring for packets to a server of interest and then forwarding or dropping packets based on a conversation identifier.

Neither of the applied references shows or suggests this claimed functionality of forwarding or dropping a packet to a particular server of interest in dependence upon whether the packet is part of an existing conversation between the client sending the packet and the server of interest by reference to persistent information included in the packet. For an obviousness rejection to be proper, the Patent Office must meet the burden of establishing a *prima facie* case of obviousness. The Patent Office must meet the burden of establishing that all elements of the invention are disclosed in the cited publications or otherwise obvious. In re Sang Su Lee, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002). This burden has not been met here.

In the Primak Patent, every request is routed to a specified server. See Primak at col 6, line 35, *et seq*. In fact, the pending Office Action concedes this point at page 6:

> Although Primak shows substantial features of the claimed invention as explained above, he does not explicitly show dropping the packet if the packet is deemed to be an undesirable packets.

The Canion Application also fails to show or suggest the feature of forwarding or dropping packets in dependence upon whether the packets are part of an existing conversation. To be sure, the Canion Application does suggest dropping packets. See Canion Application at paragraph [0185]. The packets are dropped depending upon whether they are deemed to be part of an attack. In contradistinction, the present claimed invention forwards or drops a packet depending on whether it is part of an existing conversation by reference to persistent information in the packet.

Thus, specific features of the claims are not found in the applied references.

Nor would this feature be obvious: the Primak Patent makes not suggestion of packet dropping—all packets are routed; and the Canion Application drops packet using conventional firewall-type analysis not based on being part of a conversation, or not.

Moreover still other claimed features are absent from the applied references.

Each of claims 1, 11, 17, and 22 requires determining if the packet is destined for a server of interest by reference to a destination address of the packet. In contrast, the Primak Patent teaches to route packets to a server in dependence upon a Session ID. See Primak Patent at col. 8, lines 45-48. Thus, the claims are further distinguishable from the applied combination

The context for this difference between the claimed invention and the Primak system is clear when one recognizes that the Primak Patent is concerned with load balancing between servers. Thus, incoming packets are not addressed to a particular server so that packets, or client requests, can be distributed among the servers to load balance. In contrast, the present invention is concerned with protecting a particular "server of interest" and thus routes packets based on the packet destination address field.

Thus, the inventions of the independent claims are distinguishable on another point.

Arguments relative to whether claims 4, 12, 20, and 23 are unpatentable over Primak Patent in view of Canion Application in further view of the Bull Patent:

Claim 4 further describes how the "conversation identifier" is generated. It requires the use of a deterministic function with a sequence number, persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function. Claims 12, 20, and 23 have similar features.

The pending Office Action at page 11 argues:

60]. Giving the teaching of Bull et al, a person of ordinary skill in the art would have readily recognized the desirability and the advantage of modifying Primak et al by employing the system of Bull et in order to generate a unique value that identifies a client session and to verify the integrity of the response coming from the server [Col. 6, lines 39-50 and col. 7, lines 29-35].

It is respectfully asserted that the inclusion of such a value would not have been desirable or advantageous to the Primak system. The Primak system is directed to distributing content requests from clients among servers storing that content. See Primak Patent at col. 5, line 60-col. 6, line 8.

One skilled in the art at the time of the invention would not have found it obvious or even desirable to "verify the integrity of the response coming from the server" as argued in the Office Action. The objective of Primak is dealing with large numbers of request from clients, not client verification of server integrity. In short, Primak is not concerned with any verification at the client, but instead focuses on server system scaling.

Moreover, there is no suggestion in the Primak and/or Bull Patents to forward or drop packets based on a conversation identifier generated based on a "preprovided secret value" and "values extracted from the packet" as claimed.

Thus, these claims are further distinguishable over references.

Arguments relative to whether claim 9 is unpatentable over Primak Patent in view of Canion Application in further view of the Bull Patent:

Claim 9 requires " determining if time has elapsed more than a predetermined threshold since a time of first observation was recorded for the [conversation identifier], if the extracted [conversation identifier] and the independently generated [conversation identifier] are deemed to be the same and dropping the packet if the time has elapsed more than the predetermined threshold event though the extracted [conversation identifier] and the independently generated [conversation identifier] are deemed to be the same."

The pending Office Action argues at page 13:

> As per claim 9, Primak et al as modified teach the invention, wherein the method further comprises determining if time has elapsed more than a predetermined threshold since a time of first observation was recorded for the nonce, if the extracted nonce and the independently generated nonce are deemed to be the same [col. 9, lines 20-67].

However, the cited section of the Primak Patent does not seem to suggest that a packet should be dropped based on age of the conversation identifier in spite of the existence of a match for the conversation identifiers, as claimed. In short, the pending Office Action does not assert that the requirements of the claim are met by the reference and the reference does not show or suggest those requirements.

The Primak Patent does suggest performing load balancing based on last login time:

> nected to the last accessed application server. If the replication latency of the two databases **42***a* and **42***b* (the period of time it takes to copy updated records from one database to the other) is less than the time elapsed between the client's last access time and the client's current login time (i.e., a session interval), the dynamic content router **10** determines that the current session server can process the client's requests and appropriately updates the last accessed application server field and the last access time field of the client's content record. That is, the last accessed application

However, packets are not dropped based on an age criteria as claimed.

Thus, this claim is further distinguishable.

For the foregoing reasons, Applicants believe that the pending rejections should be withdrawn, and that the present application should be passed to issue. Should any questions arise, please contact the undersigned.

Respectfully submitted,

Houston Eliseeva LLP

By /grant houston/
J. Grant Houston
Registration No.: 35,900
4 Militia Drive, Ste. 4
Lexington, MA 02421
Tel.: 781-863-9991
Fax: 781-863-9931

Date: November 8, 2007

Claims Appendix

a.) Listing of Claims

1. (Previously presented) In a routing device, a method of operation comprising:

receiving a packet sent by a client device;

determining if the packet is destined for a server of interest by reference to a destination address of the packet;

if the packet is not destined for the server of interest, routing the packet to its destination;

if the packet is determined to be destined for the server of interest, independently determining whether said packet is a part of a conversation between the client device and the server of interest based at least in part on persistent information included in said packet; and

handling the packet based at least in part on the result of said independent determination by forwarding the packet to the server of interest if the packet is deemed to be a part of a conversation between the client device and the server and dropping the packet if the packet is deemed to be an undesirable packet.

2. (Original) The method of claim 1, wherein said independent determination comprises independently verifying a conversation identifier included in said packet based at least in part on other information included in said packet.

3. (Original) The method of claim 2, wherein said independent verification comprises

independently regenerating the conversation identifier using at least said other information included in said packet; and

comparing the independently re-generated conversation identifier with the included conversation identifier.

4. (Original) The method of claim 3, wherein said conversation identifier is a nonce, and said independent re-generation comprises independently re-generating the nonce using a

deterministic function with a sequence number of the nonce and a plurality of persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function.

5. (Original) The method of claim 4, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

6. (Original) The method of claim 4, wherein the method further comprises at least one of receiving into said routing device said secret value, and equipping/configuring said routing device with said deterministic function.

7. (Original) The method of claim 4, wherein said independent generation is performed using a selected one of a message authentication code function and an universal hash function.

8. (Original) The method of claim 4, wherein the method further comprises recording a time of first observation for the nonce if the nonce is a newly observed nonce.

9. (Previously presented) The method of claim 8, wherein the method further comprises determining if time has elapsed more than a predetermined threshold since a time of first observation was recorded for the nonce, if the extracted nonce and the independently generated nonce are deemed to be the same and dropping the packet if the time has elapsed more than the predetermined threshold event though the extracted nonce and the independently generated nonce are deemed to be the same.

10. (Cancelled)

11. (Previously presented) In a server and network, a method of operation comprising:

generating an independently verifiable conversation identifier for a packet destined for a client device, using at least persistent information that will be included in said packet;

including the independently verifiable conversation identifier with said packet for use by the client device to include in a subsequent packet sent by the client device destined for the server;

transmitting said independently verifiable conversation identifier included in the packet to said client device; and

determining whether to forward or drop the packet through a network in response to the conversation identifier to protect the network against undesirable packets by determining if the packet is destined for the server by reference to a destination address of the packet, if the packet is not destined for the server routing the packet to its destination, if the packet is determined to be destined for the server determining whether the packet is a part of a conversation between the client device and the server based at least in part on the persistent information included in said and forwarding the packet to the server if the packet is deemed to be a part of a conversation between the client device and the server and dropping the packet if the packet is deemed to be an undesirable packet.

12. (Original) The method of claim 11, wherein said generation of an independently verifiable conversation identifier comprises:

generating a sequence number for a nonce; and

generating the nonce as the independently verifiable conversation identifier for the packet using a deterministic function with the sequence number, a plurality of persistent field values of the packet, and a secret value as input values to the deterministic function.

13. (Original) The method of claim 12, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

14. (Cancelled)

15. (Cancelled)

16. (Cancelled)

17. (Previously presented) A routing apparatus comprising:

an interface to receive a packet sent by a client device destined for a server; and

a function unit coupled to the interface to independently determine whether said packet is a part of a conversation between the client and the server based at least in part on persistent information included in the packet, and output a packet disposition signal based at least in part on the result of said independent determination

wherein the function unit determines if the packet is destined for the server by reference to a destination address of the packet; if the packet is not destined for the server, routing the packet to its destination; if the packet is determined to be destined for the server, independently determining whether said packet is a part of a conversation between the client device and the server based at least in part on the persistent information included in the packet; wherein the packet disposition signal causes the routing device to forward the packet to the server if the packet is deemed to be a part of conversation between the client device and the server and drop the packet if the packet is deemed to be an undesirable packet.

18. (Original) The routing apparatus of claim 17, wherein said function unit is to designed to make said independent determination by independently verifying a conversation identifier included in said packet based at least in part on other information included in said packet.

19. (Original) The routing apparatus of claim 18, wherein said function unit comprises

an identifier generator to independently regenerate the conversation identifier using at least said other information included in said packet; and

a comparator coupled to the identifier generator to compare the independently re-generated conversation identifier with the included conversation identifier.

20. (Original) The routing apparatus of claim 19, wherein said conversation identifier is a nonce, and said identifier generator is designed to independently re-generate the nonce using a deterministic function with a sequence number of the nonce and a plurality of persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function.

21. (Original) The routing apparatus of claim 20, wherein said identifier generator comprises a deterministic function.

22. (Currently amended) A server comprising:

at least one processor; and

a communication interface coupled to the processor to transmit packets to one or more client devices on behalf of the processor including

a generator to generate an independently verifiable conversation identifier for a packet destined for one of said one or more client devices, using at least persistent information that will be included in said packet,

a summing unit to insert the independently verifiable conversation identifier with said packet for use by the particular client device to include in a subsequent packet sent by the client device destined for the server, and

a transmitter to transmit said independently verifiable conversation identifier included packet to said particular client device

wherein a router determines if the packet is destined for the server by reference to a destination address of the packet; if the packet is not destined for the server, routing the packet to its destination; if the packet is determined to be destined for the server, independently determining whether the packet is a part of a conversation between the client device and the server based at least in part on the independently verifiable conversation identifier included in said packet; wherein the routing device to forwardes

the packet to the server if the packet is deemed to be a part of the conversation between the client device and the server and dropping the packet if the packet is deemed to be an undesirable packet..

23. (Previously presented) The server of claim 22, wherein said generator comprises

a counter to generate a sequence number for a nonce; and

a deterministic function unit to generate the nonce as the independently verifiable conversation identifier for the packet using the sequence number, a plurality of persistent field values of the packet, and a secret value as input values.

24. (Previously presented) The server of claim 23, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

25. (Previously presented) The server of claim 23, wherein said deterministic function is a selected one of a message authentication code function and a universal hash function.

26. (Cancelled)

27. (Cancelled)

28. (Cancelled)

29. (Cancelled)

30. (Cancelled)

31. (Cancelled)

32. (Previously presented) The routing apparatus of claim 17, wherein said function unit drops packets that are not part of the conversation to protect the server against receipt of undesirable packets.

Evidence Appendix

None

Related Proceedings Appendix

None